UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/982,711 | 10/18/2001 | Taizo Shirai | 09812.0590-00000 | 8666 |

| | |
|---|---|
| 22852          7590          01/28/2010 | EXAMINER |
| FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP | KHOSHNOODI, NADIA |
| 901 NEW YORK AVENUE, NW | |
| WASHINGTON, DC 20001-4413 | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 01/28/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 09/982,711 | SHIRAI ET AL. |
| | Examiner | Art Unit | |
| | NADIA KHOSHNOODI | 2437 | |

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on <u>11 January 2010</u>.

2a) ☐ This action is **FINAL**.      2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) <u>1,5,6,8,12,13,17,21,22,24,28,29,31 and 32</u> is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1,5,6,8,12,13,17,21,22,24,28,29,31 and 32</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>24 January 2006</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a) ☒ All    b) ☐ Some * c) ☐ None of:

       1. ☒ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

## DETAILED ACTION

### Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection.  Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114.  Applicant's submission filed on 1/11/2010 has been entered.

### Response to Amendments

Applicant's amendments/arguments filed 5/15/2009 with respect to pending claims 1, 5-6,

8, 12-13, 17, 21-22, 24, 28-29, 31, and 32 have been fully considered but are moot in view of the

new ground(s) of rejection.

### Claim Objections

Claims 1, 8, 17, 24, and 31-32 are objected to because of the following informalities: in

the second to last limitation of each of these claims, Applicants make reference to "a memory

unit identifier" which is has already been introduced in the first limitation of each of these

claims.  It seems that Applicants intended to refer back to the previously introduced memory unit

identifier.  Appropriate correction is required.

### Claim Rejections - 35 USC § 103

I.      The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains.  Patentability shall not be negatived by the
> manner in which the invention was made.

II.     Claims 1, 8, 17, 24, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Nagai et al., US Pub. No. 2005/0185547 and further in view of Pebley et al., US Patent No.

6,154,840.

As per claims 1, 17, and 31:

        Nagai et al. substantially teach the device/method/computer readable medium

comprising: a memory unit containing data, including content data (par. 132) and a block

permission table defining memory-access control information (par. 266 and par. 269 and Fig.

23), and an integrity check value for the block permission table generated based on a memory

unit identifier (par. 148 and par. 155), the memory unit having a data storage area comprising a

plurality of blocks, each of the blocks comprising M sectors from a first to a M-th sector with

each sector having a predetermined data capacity, where M represents a natural number (par.

137); a processing unit for dividing content data into separate content data portions, for storing

each of the separate content data portions in a different sector within a first data block of the data

storage area (par. 178 and Fig. 5, elements 502 & 507); and for a security header corresponding

to the content data in a second data block of the data storage area, wherein the first data block is

different from the second data block (par. 138, lines 12-22 and Fig. 5, element 503); an integrity

check unit for checking the integrity of the block permission table based on the integrity check

value generated based on a memory unit identifier (par. 155), wherein the security header stored

in the second data block includes each encryption key used for encryption of the first data block
(par. 152, lines 1-7).

Not explicitly disclosed is a cryptosystem unit for performing sector-level encryption by
using a different encryption key for each sector of the first data block to execute encryption
processing on the content data portion to be stored in each of the sector. However, Pebley et al.
teach a different key may be created and used to encrypt/decrypt each portion of the content file
which was broken up into blocks (col. 4, lines 32-67). Therefore, it would have been obvious to
a person in the art at the time the invention was made to modify the method disclosed in Nagai et
al. to use a different key to encrypt/decrypt each sector. This modification would have been
obvious because a person having ordinary skill in the art, at the time the invention was made,
would have been motivated to do so since Pebley et al. suggest that using a different key per
sector strengthens the level of confidentiality for the document in col. 4, lines 32-67 and col. 5,
lines 26-32.

As per claims 8, 24, and 32:

Nagai et al. substantially teach the information recording device/method for executing
processing/computer readable medium comprising: a memory unit containing data, including
encrypted content data (par. 122) and a block permission table defining memory-access control
information (par. 266 and par. 269 and Fig. 23), and an integrity check value for the block
permission table generated based on a memory unit identifier (par. 148 and par. 155), the
memory unit having a data storage area comprising a plurality of blocks, each of which
comprising M sectors form a first sector to a M-th sector which each have a predetermined data
capacity, where M represents a natural number (par. 137); a processing unit for reading

encrypted content data portions which together comprise encrypted content data, wherein each

encrypted content data portion has been encrypted and is read from a different sector within a

first data block of the data storage area (par. 178 and Fig. 5, elements 502 and 507) and for

reading a security header corresponding to the encrypted content data from a second data block

of the storage area, wherein the first data block is different from the second data block (par. 138,

lines 12-22 and Fig. 5, element 503); and an integrity checking unit for checking the integrity of

the block permission table based on the integrity check value generated based on a memory unit

identifier (par. 155), wherein the security header read from the second data block includes the

encryption key used to encrypt each encrypted content data portion read from the first data block

(par. 152, lines 1-7).

Not explicitly disclosed is wherein each encrypted content data portion has been

encrypted using a different encryption key and performing sector level decryption by using

different decryption keys. However, Pebley et al. teach a different key may be created and used

to encrypt/decrypt each portion of the content file which was broken up into blocks (col. 4, lines

32-67). Therefore, it would have been obvious to a person in the art at the time the invention

was made to modify the method disclosed in Nagai et al. to use a different key to encrypt/decrypt

each sector. This modification would have been obvious because a person having ordinary skill

in the art, at the time the invention was made, would have been motivated to do so since Pebley

et al. suggest that using a different key per sector strengthens the level of confidentiality for the

document in col. 4, lines 32-67 and col. 5, lines 26-32.

III.     Claims 5-6, 12-13, 21-22, and 28-29 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Nagai et al., US Pub. No. 2005/0185547 and Pebley et al., US Patent No.

6,154,840, as applied to claims 1, 8, 17, and 24 above, and further in view of Dilkie et al., United

States Patent No. 6,341,164.

As per claims 5 and 21:

      Nagai et al. and Pebley et al. substantially teach an information recording device and

method of claims 1 and 17. Not explicitly disclosed is the information recording device and

method wherein, in said cryptosystem unit, the encryption processing is executed as single-DES

encryption processing using different encryption keys for each sector of the first data block.

However, Dilkie et al. teaches the use of a single-DES encryption processing. Therefore, it

would have been obvious to a person in the art at the time the invention was made to modify the

device/method disclosed in Nagai et al. to use single-DES for the encryption processing. This

modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since it is suggested by Dilkie

et al. in col. 2, lines 48-54.

As per claims 6 and 22:

      Nagai et al. and Pebley et al. substantially teach an information recording device and

method, as applied to claims 1 and 17 above. Not explicitly disclosed is the information

recording device wherein, in said cryptosystem unit, the encryption processing for the first sector

to the M-th sector is executed as triple-DES encryption processing using at least two different

encryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES

encryption processing. Therefore, it would have been obvious to a person in the art at the time

the invention was made to modify the device/method disclosed in Nagai et al. to use triple-DES

for the encryption processing. This modification would have been obvious because a person

having ordinary skill in the art, at the time the invention was made, would have been motivated

to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 12 and 28:

Nagai et al. and Pebley et al. substantially teach an information recording device and

method of claims 8 and 24. Not explicitly disclosed is an information playback device and

method wherein, in said cryptosystem unit, the decryption processing is executed as single-DES

decryption processing using different decryption keys for the sectors. However, Dilkie et al.

teaches the use of a single-DES encryption processing. Therefore, it would have been obvious to

a person in the art at the time the invention was made to modify the device/method disclosed in

Nagai et al. to use single-DES for the encryption processing. This modification would have been

obvious because a person having ordinary skill in the art, at the time the invention was made,

would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 13 and 29:

Nagai et al. and Pebley et al. substantially teach an information playback device and

method, as applied to claims 8 and 24 above. Not explicitly disclosed is the information

playback device wherein, in said cryptosystem unit, the decryption processing for the first sector

to the M-th sector is executed as triple-DES decryption processing using at least two different

decryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES

decryption processing. Therefore, it would have been obvious to a person in the art at the time

the invention was made to modify the device/method disclosed in Nagai et al. to use triple-DES

for the decryption processing. This modification would have been obvious because a person

having ordinary skill in the art, at the time the invention was made, would have been motivated

to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.


## Conclusion

 Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825.

The examiner can normally be reached on M-F: 8:00-4:30.

 If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

 Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


        /Nadia  Khoshnoodi/
        Examiner, Art Unit 2437
        1/25/2010
NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437